Securing Online Gaming User Accounts
Copyright

© 2013 VASCO Data Security. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security Inc.

Trademarks

MYDIGIPASS.com, DIGIPASS & VACMAN are registered trademarks of VASCO Data Security. All other trademarks or trade names are the property of their respective owners. Any trademark that is not owned by Vasco that appears in the document is only used to easily refer to applications that can be secured with authentication solutions such as the ones discussed in the document. Appearance of these trademarks in no way is intended to suggest any association between these trademarks and any Vasco product or any endorsement of any Vasco product by these trademarks’ proprietors. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.
Table of Contents

Executive Summary .................................................................................................................. 3
Growing online gaming market .............................................................................................. 3
Virtual economies, real money issues .................................................................................... 4
Protect the business by protecting users ............................................................................. 5
Allow us to help you make the right decision ....................................................................... 6
Securing Online Gaming User Accounts

Executive Summary

Online gaming is a multi-billion dollar business. When hackers attack, users, online gaming developers and publishers are all negatively affected. VASCO helps protect the online gaming business by guarding users’ accounts against unauthorized access and theft of gaming assets.

Growing online gaming market

Your customers’ identities are as safe as you want them to be. Most people have many online accounts, but don’t spend much thought or time on managing the security of the logins information and passwords.

Traditional online games have a substantial customer base. Massively Multiplayer Online Game (MMOG) popularity is growing the most, supporting hundreds of millions of simultaneous players. MMOGs contribute a significant percentage of revenue to the gaming industry. By linking traditional disc-based games with online versions, gaming publishers are improving the gaming experience via MMOG.
Virtual economies, real money issues

MMOG introduced a new phenomenon: virtual economies. Players can accumulate virtual currency that is used to purchase new capabilities or new paraphernalia — all in the name of improving their online personas in the game. Gamers create online gaming accounts to store acquired materials and gaming credits. This is a big opportunity for fraudsters who hack into gamers' accounts, strip players of their gaming credits, acquire game paraphernalia, then resell these virtual assets to other gamers. *This process is known as “gold farming.”*

Another growing trend is cyber-bullying. Hackers steal users’ credentials and wreak havoc in the online world. For example, a hacker can disrupt the game by violating its code of conduct. The result is a poor customer experience for all game users, which can result in subscriber churn and revenue loss.

Another growing trend is account sharing. Although not as damaging to other players as the other issues described above, account sharing has an immediate impact on subscription revenues. A single account is accessed by multiple users to pool their collective knowledge and experiences, for example, to make it to the next game level or acquire additional capabilities. The result is lost subscription revenue. This issue is increasingly important when gaming companies’ monthly MMOG revenues are declining, as shown below (Source: SuperData Research).

As the online gaming population increases, but average revenue per user declines, further monetization is clearly needed. Secure
accounts result in more positive customer experiences which, in turn, foster user stickiness. This opens up the opportunity to cross-sell additional gaming assets to both pay-to-play and free-to-play users. And, a convenient way to cross-sell is to provide one secure credential and secure portal to enable users to access different game sites.

Protect the business by protecting users

VASCO helps protect the online gaming business by guarding user accounts from gold farming, cyber-bullying and account sharing, while making it easier to generate more revenues by cross-selling game assets. VASCO offers a portfolio of authentication solutions to address different business models and the device preferences of the user community.

Authentication can be completed with smartphones, secure chipsets, or even SMS-based authentication, particularly for games that have large customer bases in countries where smartphone penetration is low.

Traditional client-server

Several online gaming developers and publishers already use VASCO to secure online gaming platforms by using a client-server combination of DIGIPASS GO 6 tokens, VACMAN Controller and IDENTIKEY server solutions.

DIGIPASS GO 6 is a physical, one-button authenticator that dynamically generates one-time passwords (OTP) versus relying on hack-prone static passwords. OTPs are only used once and expire quickly, for example every 32 seconds, making it difficult for anyone trying to breach a user’s account. The hardware authenticator is customizable using the gaming publishers’ logos or artwork to enhance brand recognition. DIGIPASS GO 6 is just one of the many client OTP generation device options that are part of VASCO’s portfolio.

VACMAN Controller is the authentication engine that verifies all login requests from authorized DIGIPASS users. It is the backend portion of the solution that verifies the OTP generated by the DIGIPASS client. VACMAN Controller is a library that integrates into gaming publishers’ existing environments.
IDENTIKEY Server is the complete server solution that provides the operations, administration and management (OA&M) and provisioning component of the solution. The authentication engine of IDENTIKEY Server is the VACMAN Controller. The IDENTIKEY Server software runs on Microsoft Server operating systems and Linux enterprise operating system software.

Another option gaming publishers have is DIGIPASS Plus. DIGIPASS Plus is a technology and business model where the user can have one OTP client device and that single device has two secrets that can be used for separate applications. The gaming publisher can have security for their fat client application where the VACMAN Controller is integrated as part of their OA&M backend system. At the same time, the same user can securely access any web application the gaming publisher may have through MYDIGIPASS.COM – all of this using the same OTP client device which makes it convenient for the user.
Securing Online Gaming User Accounts

Federated or Single Sign-On (SSO)

Online gaming publishers can also conveniently extend security for their users to other gaming or online assets in their portfolios. For example, MMOG users of a medieval-time theme game can securely access a futuristic war theme game. Or, free-to-play users can upgrade accounts to a pay-to-play game using secure access.

Different combinations of DIGIPASS client OTP generation hardware and software tokens can be used depending on the backend infrastructure configuration.

Examples of DIGIPASS client OTP generation tokens are:
- DIGIPASS hardware token
- MYDIGIPASS.COM mobile device software application with human-readable OTP and QR code scanner
- DIGIPASS Embedded System Solution such as Intel Intelligent Protection Technology where the OTP is generated directly from the secure chipset on the PC
- SMS

Different backend infrastructure options are available depending on the technical and business requirements, described below. The key component of the backend infrastructure in this model is the use of a federation solution. Federation is what enables a single user to securely access multiple applications with a single authentication request.

**Full cloud-hosted backend infrastructure:**

MYDIGIPASS.COM is an end-to-end authentication solution that includes the functions of federation, OA&M and authentication verification. The cloud infrastructure is fully operated and managed by VASCO. The solution leverages DIGIPASS as a Service (DPS) that provides the OA&M function. VACMAN Controller is the authentication engine.

The online gaming publisher wants to authenticate both downloadable fat client games, as well as HTML browser-based games, using a single authentication engine. A user can then employ the same DIGIPASS authentication device across all gaming applications whether it is accessed in a PC application or in a browser window.

**Hybrid federation:** In this scenario, the online gaming publisher wants to authenticate both downloadable fat client games, as well as HTML browser-based games, using a single authentication engine. A user can then employ the same...
DIGIPASS authentication device across all gaming applications whether it is accessed in a PC application or in a browser window.

Allow us to help you make the right decision

VASCO is the leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. We also offer Professional Services to help speed your implementation and leverage our expertise to aid gaming companies in their go-to-market plans to roll out authentication to their user base. Contact us for any questions and allow us to help you make the right decision that balances security, ease-of-use and cost for your business and your valuable customers. You can visit us at www.vasco.com for more information.
About VASCO

VASCO designs, develops, markets and supports MYDIGIPASS.COM™, DIGIPASS®, DIGIPASS PLUS™, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

<table>
<thead>
<tr>
<th>BRUSSELS (Europe)</th>
<th>BOSTON (America)</th>
<th>SYDNEY (Pacific)</th>
<th>SINGAPORE (Asia)</th>
</tr>
</thead>
<tbody>
<tr>
<td>+32.2 609 97 00</td>
<td>+1.508.366.3400</td>
<td>+61.2.8061.3700</td>
<td>+65.6 32 30906</td>
</tr>
<tr>
<td><a href="mailto:info-europe@vasco.com">info-europe@vasco.com</a></td>
<td><a href="mailto:info-usa@vasco.com">info-usa@vasco.com</a></td>
<td><a href="mailto:info-australia@vasco.com">info-australia@vasco.com</a></td>
<td><a href="mailto:info-asia@vasco.com">info-asia@vasco.com</a></td>
</tr>
</tbody>
</table>